Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] 1. A method for securing software to reduce unauthorized use, the method comprising:
obtaining registration information corresponding to at least one authorized secondary device;
generating an authentication code based on the registration information;
associating the authentication code with the software;
transferring the software to a primary user device;
determining whether a current secondary device is authorized based on the authentication code associated with the software and registration information associated with the current secondary device; and
controlling access to the software by the current secondary device based on whether the current secondary device is authorized.

[c2] 2. The method of claim 1 wherein the software comprises digital content selected from the group consisting of data representing music, data representing video, instructions executable by a computer, code for an application program, code for an operating system component, code for a game, data representing a movie, data

representing graphics, data representing watermarked works, data representing a magazine, and data representing a book.

[c3] 3. The method of claim 1 wherein the step of transferring the software is performed before the steps of obtaining registration information, generating an authentication code, and associating the authentication code.

[c4] 4. The method of claim 1 wherein the step of transferring comprises transferring the software from a computer readable storage medium.

[c5] 5. The method of claim 1 wherein the step of transferring comprises transferring the software electronically.

[c6] 6. The method of claim 1 wherein the step of transferring comprises transferring the software from a network.

[c7] 7. The method of claim 1 wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed by an authorized representative entity.

[c8] 8. The method of claim 7 wherein the authorized representative entity is installed on or in the primary user device.

[c9] 9. The method of claim 7 wherein the authorized repre-

sentative entity is installed on or in the current secondary user device.

[c10] 10. The method of claim 7 wherein an authorized representative entity is installed on or in the primary device and an authorized representative entity is installed on or in the current secondary user device.

[c11] 11. The method of claim 7 wherein the authorized representative entity is remotely located relative to the primary and secondary devices.

[c12] 12. The method of claim 1 further comprising:
obtaining registration information corresponding to the primary user device;
generating an authentication code based on the registration information;
associating the authentication code with the software; and
controlling access to the software by a current primary user device based on whether the current primary user device is authorized.

[c13] 13. The method of claim 1 further comprising:
installing an authorized representative entity on or in at least one of the primary and secondary user devices.

[c14] 14. The method of claim 13 wherein the authorized rep-

resentative entity performs the step of controlling access to the software by the current secondary device.

[c15] 15. The method of claim 13 wherein the authorized representative entity is installed on or in the primary user device and wherein controlling access comprises preventing the software from being transferred to the current secondary device.

[c16] 16. The method of claim 13 wherein the authorized representative entity is installed on or in the primary user device and wherein controlling access comprises:
modifying the software to generate reduced quality software; and
transferring the reduced quality software to the current secondary device.

[c17] 17. The method of claim 1 wherein the primary user device comprises a computer and the at least one secondary device comprises a digital audio player.

[c18] 18. The method of claim 1 wherein the step of controlling access to the software is performed by the current secondary device.

[c19] 19. The method of claim 1 wherein the step of controlling access to the software is performed by the primary user device.

[c20] 20. The method of claim 1 wherein the step of controlling access to the software comprises transferring the authentication code corresponding to the at least one authorized secondary device along with the software to the current secondary device.

[c21] 21. The method of claim 1 wherein the step of controlling access to the software comprises determining whether the current secondary device has an operable authorized representative entity.

[c22] 22. The method of claim 21 further comprising:
installing an authorized representative entity on or in the current secondary device if an operable authorized representative entity is not detected.

[c23] 23. The method of claim 21 wherein the step of controlling access determines that the current secondary device includes an authorized representative entity installed on or in the device, the method further comprising:
transferring the software to the current secondary device; and
controlling access to the software on the current secondary device using the authorized representative entity installed on or in the current secondary device.

[c24] 24. The method of claim 1 wherein the step of obtaining

registration information comprises prompting the user to identify at least one secondary device.

[c25] 25. The method of claim 1 wherein the step of obtaining registration information comprises automatically obtaining registration information associated with at least one secondary device.

[c26] 26. The method of claim 1 wherein the step of determining is performed by an authorized representative entity installed on the primary user device in communication with the current secondary device.

[c27] 27. The method of claim 26 wherein the current secondary device is in wireless communication with the primary user device.

[c28] 28. The method of claim 27 wherein the current secondary device is a personal digital assistant.

[c29] 29. The method of claim 1 wherein the step of controlling access to the software comprises preventing transfer of at least a portion of the software to the current secondary device.

[c30] 30. The method of claim 1 wherein the step of controlling access to the software comprises preventing the current secondary device from utilizing the software.

[c31] 31. The method of claim 1 wherein the step of controlling access comprises providing a second file type for use with the secondary device.

[c32] 32. The method of claim 1 wherein the steps of obtaining, generating, and associating are performed by the primary user device and the steps of determining and controlling are performed by the current secondary device.

[c33] 33. The method of claim 1 further comprising encrypting the authentication code.

[c34] 34. The method of claim 1 further comprising associating an identifier with the software to trigger authentication by an authorized representative entity.

[c35] 35. The method of claim 1 further comprising disabling means for generating the authentication code.

[c36] 36. The method of claim 1 wherein the software is included in a computer readable storage medium.

[c37] 37.The method of claim 1 wherein the authentication code at least partially corresponds to a secondary device manufacturer.

[c38] 38.The method of claim 1 wherein the authentication

code at least partially corresponds to a specific type of secondary device.

[c39] 39. The method of claim 1 further comprising securing the authentication code to hinder user tampering.

[c40] 40. A method for securing software having at least one associated authentication code to reduce unauthorized use, the method comprising:
intercepting a request to access the software;
determining whether an authorized representative entity is available to authenticate a user device for which software access is requested;
if an operational authorized representative entity is available, using the authorized representative entity to determine if the user device for which software access is requested is authorized based on the at least one authentication code and providing access to the software if the user device is authorized; and
if an operational authorized representative entity is not available, installing an authorized representative entity from the software and determining whether the user device is authorized using the installed authorized representative entity.

[c41] 41. The method of claim 40 wherein the software comprises digital content selected from the group consisting

of data representing music, data representing video, instructions executable by a computer, code for an application program, code for an operating system component, code for a game, data representing a movie, data representing graphics, data representing watermarked works, data representing a magazine, and data representing a book.

[c42] 42. The method of claim 40 wherein the step of intercepting comprises intercepting a request to transfer the software from a primary user device to a secondary user device.

[c43] 43. The method of claim 40 wherein the step of intercepting comprises intercepting a request to utilize the software.

[c44] 44. The method of claim 40 wherein the step of determining comprises determining whether an authorized representative entity is installed on or in a secondary device.

[c45] 45. The method of claim 40 further comprising transferring the software to a secondary device if the secondary device is determined to be authorized based on the at least one authentication code.

[c46] 46. The method of claim 45 wherein a primary device

determines whether the secondary device is authorized.

[c47] 47. The method of claim 45 wherein a remote authorized representative entity determines whether the secondary device is authorized.

[c48] 48. A method for securing software to reduce unauthorized use, the method comprising:
associating an identifier with the software to request authentication;
distributing the software to a user;
detecting the identifier associated with the software to activate authentication using an authorized representative installed on a primary user device;
obtaining registration information associated with at least one secondary device;
generating an authentication code based on the registration information;
linking the authentication code to the software; andcontrolling access to the software by a secondary device based on the authentication code.

[c49] 49. The method of claim 48 wherein the step of obtaining registration information comprises prompting a user to identify at least one secondary device.

[c50] 50. The method of claim 48 wherein the software com-

prises digital content selected from the group consisting of data representing music, data representing video, instructions executable by a computer, code for an application program, code for an operating system component, code for a game, data representing a movie, data representing graphics, data representing watermarked works, data representing a magazine, and data representing a book.

[c51] 51. The method of claim 48 wherein the step of obtaining registration information comprises automatically obtaining hardware information associated with the secondary device.

[c52] 52.The method of claim 48 wherein the authentication code at least partially corresponds to a secondary device manufacturer.

[c53] 53.The method of claim 48 wherein the authentication code at least partially corresponds to a specific type of secondary device.

[c54] 54. The method of claim 48 wherein the step of linking comprises embedding the authentication code within the software.

[c55] 55. The method of claim 48 wherein the step of linking comprises modifying the software based on the authen-

tication code for use by an authorized secondary device.

[c56] 56. The method of claim 48 wherein the step of controlling access to the software comprises preventing the software from being transferred to an unauthorized secondary device.

[c57] 57. The method of claim 48 wherein the step of controlling access to the software comprises preventing unauthorized secondary devices from utilizing the software.

[c58] 58. The method of claim 48 wherein the steps of obtaining registration information, generating an authentication code, and linking the authentication code are preformed prior to the step of distributing the software to a user.

[c59] 59. The method of claim 48 wherein the step of distributing the software comprises distributing the software on a computer readable storage medium.

[c60] 60. The method of claim 48 wherein the step of distributing the software comprises electronically distributing the software.

[c61] 61. The method of claim 48 further comprising installing an authorized representative entity on at least one of the primary and secondary devices.

[c62] 62. The method of claim 61 wherein the authorized representative entity is installed from a computer readable storage medium.

[c63] 63. The method of claim 61 wherein the authorized representative entity is installed from a network.

[c64] 64. The method of claim 48 wherein the step of controlling access to the software comprises preventing the software from being transferred to a secondary device unless the secondary device has an authorized representative entity installed.

[c65] 65. The method of claim 48 wherein the step of obtaining registration information comprises automatically obtaining registration information associated with the primary device and at least one secondary device.

[c66] 66. The method of claim 48 wherein the step of controlling access comprises restricting access to the software by the secondary device unless the secondary device can be automatically identified by the authorized representative installed on the primary user device.

[c67] 67. The method of claim 48 wherein the step of controlling access comprises providing limited access by the secondary device if the secondary device can not be au-

tomatically identified by the authorized representative entity installed on the primary user device.

[c68] 68. The method of claim 48 wherein the step of controlling access comprises providing a second file type for use with the secondary device.

[c69] 69. The method of claim 48 wherein the primary user device comprises a computer and wherein the secondary device comprises a digital audio player.

[c70] 70. The method of claim 48 wherein the secondary device comprises a cellular telephone.

[c71] 71. The method of claim 48 wherein the secondary device comprises a portable user device.

[c72] 72. The method of claim 48 wherein the authorized representative entity installed on the primary device comprises a hardware device.

[c73] 73. The method of claim 48 wherein the authorized representative entity installed on the primary device comprises software.

[c74] 74. The method of claim 48 wherein the authorized representative entity installed on the primary device comprises hardware and software.

[c75] 75. The method of claim 48 further comprising contacting a remote authorized representative entity if the authorized representative entity is unable to authenticate the secondary device based on the authentication code.

[c76] 76. The method of claim 48 wherein the step of controlling access to the software is performed by the secondary device.

[c77] 77. The method of claim 48 wherein the step of controlling access to the software is performed by a remote authorized representative entity.

[c78] 78. The method of claim 48 wherein the step of controlling access to the software comprises modifying the software so the software is unusable.

[c79] 79. The method of claim 48 wherein the software is included in a computer readable storage medium.

[c80] 80. The method of claim 48 further comprising encrypting the authentication code.

[c81] 81. A method for reducing unauthorized use of software including digital content, the method comprising:
obtaining registration information associated with at least one portable user device;
generating at least one authentication code based on the

registration information associated with the at least one portable device;
associating the authentication code with the software;
transferring the software to a user computer;
controlling access to the software using at least one authorized representative entity to inhibit access to the software by unauthorized portable user devices.

[c82] 82. The method of claim 81 wherein the software comprises digital content selected from the group consisting of data representing music, data representing video, instructions executable by a computer, code for an application program, code for an operating system component, code for a game, data representing a movie, data representing graphics, data representing watermarked works, data representing a magazine, and data representing a book.

[c83] 83. The method of claim 81 wherein the step of obtaining registration information comprises automatically obtaining hardware information associated with the portable user device.

[c84] 84. The method of claim 81 wherein the registration information corresponds to a group of portable devices.

[c85] 85. The method of claim 81 wherein the authentication

code corresponds to a group of portable devices.

[c86] 86.The method of claim 81 wherein the authentication code at least partially corresponds to a secondary device manufacturer.

[c87] 87.The method of claim 81 wherein the authentication code at least partially corresponds to a specific type of secondary device.

[c88] 88. The method of claim 81 wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed by a remote authorized representative entity.

[c89] 89. The method of claim 81 wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed by the user computer.

[c90] 90. The method of claim 81 wherein the step of controlling access is performed by the portable user device.

[c91] 91. The method of claim 81 wherein the step of controlling access comprises:
determining if a portable user device includes an authorized representative entity; and
transferring the software to the portable user device only

if the portable user device includes an authorized representative entity.

[c92] 92. The method of claim 91 wherein the step of controlling access further comprises:
determining if the portable user device is authorized to access the software based on the at least one authentication code using the authorized representative entity on the portable device; and
controlling access to the software by the portable device using the authorized representative entity on the portable device.

[c93] 93. The method of claim 81 wherein the step of controlling access comprises modifying the software if the portable device is not authorized to access the software.

[c94] 94. The method of claim 93 wherein the step of modifying the software comprises reducing quality of content contained in the software.

[c95] 95. The method of claim 93 wherein the step of modifying the software comprises rendering the software unusable on any portable device.